Sample Audit Report

Supporting Document 1: Sample Audit Report

NIST SP 800-171 Rev. 3 Compliance Readiness Report

Client: SecurePath Tech Solutions, Inc.

Industry: Technology / SaaS

Assessment Period: Q1 2025

Assessor: B. Akintade, Snr. GRC Consultant

Executive Summary

A targeted internal readiness assessment was conducted to evaluate the client's alignment with NIST SP 800-171 Rev. 3 controls. The review included interviews with internal stakeholders, control testing, document sampling, and gap identification across 14 control families.

Key Takeaways:

- **Control Coverage:** ~68% baseline control maturity
- **High-Risk Gaps:** 7 controls lacked implementation, primarily under Access Control and System & Communications Protection
- **Recommendations:** Immediate remediation on MFA, logging practices, and audit policy documentation

Key Findings Summary

Control Family	**% Compliant**	**Priority Remediation Recommendation**
Access Control (AC)	50%	Implement granular RBAC and MFA enforcement
Audit and Accountability (AU)	60%	Develop formal audit log retention policy
System & Communications (SC)	55%	Enable data-in-transit encryption
Risk Assessment (RA)	75%	Perform annual formal risk assessment
Incident Response (IR)	80%	Finalize IR plan and conduct tabletop exercises

Next Steps

- Deliver prioritized remediation roadmap (30/60/90 day)
- Develop policy documentation for deficient domains
- Conduct user security awareness training
- Reassess for compliance alignment post-remediation

Supporting Document 2: ISO 27001-Aligned Policy Sample

Title: Information Access Control Policy

Standard Alignment: ISO/IEC 27001:2022 – Annex A.9

Purpose: To establish a control framework that governs access to organizational information and systems, minimizing the risk of unauthorized disclosure, alteration, or destruction of information.

Scope: Applies to all employees, contractors, and third-party users accessing company-owned systems, devices, or applications.

Policy Statements:

1. Access to information will be granted based on the principle of least privilege and business necessity

2. All users must authenticate using approved multi-factor authentication

3. Privileged access must be tightly controlled, reviewed quarterly, and logged for auditability

4. User accounts will be deactivated immediately upon employment termination

5. Access rights will be reviewed semi-annually by system owners

Enforcement: Non-compliance may result in disciplinary actions up to and including termination of employment and/or legal penalties.

Supporting Document 3: NIST 800-53 Rev. 5-Aligned Policy Sample

Title: System and Communications Protection Policy

Framework Reference: NIST 800-53 Rev. 5 (SC Family)

Policy Objective: To protect the integrity, confidentiality, and availability of organizational systems and communications, ensuring compliance with federal and industry cybersecurity standards.

Scope: This policy applies to all enterprise IT infrastructure, communication systems, and connected third-party platforms.

Policy Directives:

1. All system interconnections must be documented and authorized prior to implementation

2. Enforce TLS 1.2 or higher encryption on all data-in-transit across internal and external networks

3. Mobile and wireless devices must utilize approved VPN configurations

4. Inbound and outbound traffic will be monitored using intrusion detection/prevention systems

5. Split tunneling is prohibited unless explicitly authorized and monitored

Review Cadence: This policy will be reviewed annually or upon significant change to system architecture.

Supporting Document 4: Ransomware Tabletop Summary

Tabletop Exercise Report – Ransomware Incident Simulation

Client: SecurePath Tech Solutions, Inc.

Facilitator: B. Akintade, GRC Program Lead

Date: April 2024

Objectives

- Test the organization’s readiness to detect, respond to, and recover from a ransomware attack
- Identify procedural gaps in communication, decision-making, and technical response
- Validate Incident Response Plan (IRP) assumptions and cross-functional responsibilities

Scenario Summary

Simulated ransomware attack affecting internal ERP system, requiring coordinated response from IT, Legal, HR, and Executive Leadership.

Key Outcomes

- **Communication Lag:** Initial alert delayed by 28 minutes due to unclear escalation chain
- **Backups Validated:** Restoration testing succeeded within 6 hours
- **Policy Gaps:** Need for clearer guidance on media outreach and executive-level decision thresholds
- **Compliance Risk:** Absence of breach notification procedure for state-level regulators

Recommendations

- Update Incident Response Plan with communication playbooks
- Conduct quarterly IR tabletop exercises
- Formalize breach notification policy for legal/compliance team use
- Enhance endpoint detection coverage for remote users

Prepared by: Busayo (B) Akintade
Snr. GRC Consultant | Cybersecurity Compliance & Risk